REMARKS

I. Introduction

In response to the Office Action dated July 31, 2002, no claims have been cancelled, amended, or added. Claims 1-117 remain in the application. Re-examination and re-consideration of the application is requested.

II. Prior Art Rejections

A. The Office Action Rejections

In paragraphs (2)-(3) of the Office Action, claims 1, 13, 14, 16, 17, 21, 22, 40, 52, 53, 55, 56, 60, 61, 79, 91, 92, 94, 95, 99, and 100 were rejected under 35 U.S.C. §102(e) as being anticipated by Crichton et al., U.S. Patent No. 6,104,716 (Crichton). In paragraphs (4)-(5) of the Office Action, claims 3-11, 42-50, and 81-89 were rejected under 35 U.S.C. §103(a) as being unpatentable over Crichton. In paragraph (6) of the Office Action, claims 2, 28-39, 41, 67-78, 80, and 106-117 over Crichton in view of Fox et al., U.S. Patent No. 6,421,781 (Fox). In paragraph (7) of the Office Action, claims 12, 51, and 90 were rejected under 35 U.S.C. §103(a) as being unpatentable over Crichton in view of Griffiths et al., U.S. Patent No. 6,286,045 (Griffiths). In paragraph (8) of the Office Action, claims 15, 18-20, 23-25, 54, 57-59, 62-64, 93, 96-98, and 101-103 were rejected under 35 U.S.C. §103(a) as being unpatentable over Crichton in view of Coley et al., U.S. Patent No. 5,826,014 (Coley). In paragraph (9) of the Office Action, claims 26, 65, and 104 were rejected under 35 U.S.C. §103(a) as being unpatentable over Crichton in view of Raz, U.S. Patent No. 6,292,827 (Raz). In paragraph (10) of the Office Action, claims 27, 66, and 105 are rejected under 35 U.S.C. §103(a) as being unpatentable over Crichton in view of Raz and further in view of Coley.

Applicants' attorney respectfully traverses these rejections.

B. The Applicants' Claimed Invention

Independent claims 1, 40 and 79 are generally directed to a network multiplexing and tunneling system, transmission media and method. The method is representative and comprises:

(a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network;

(b) establishing a Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection;

(c) mutually authenticating each of the endpoints of the SSL TCP connection; and

(d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated.

C. The Crichton Reference

Crichton describes a lightweight secure tunneling protocol or LSTP permits communicating across one or more firewalls by using a middle server or proxy. Three proxies are used to establish an end-to-end connection that navigates through the firewalls. In a typical configuration, a server is behind a first firewall and a client behind a second firewall are interconnected by an untrusted network (e.g., the Internet) between the firewalls. A first inside firewall SOCKS-aware server-side end proxy connects to the server inside the first firewall. A second inside firewall SOCKS-aware client-side end proxy is connected to by the client inside the second firewall. Both server-side and client-side end proxies can address a third proxy (called a middle proxy) outside the two firewalls. The middle proxy is usually started first, as the other two end proxies (server and client) will initiate the connection to the middle proxy some time after they are started. Since the middle proxy is mutually addressable by both inside proxies, a complete end-to-end connection between the server and client is established. It is the use of one or more middle proxies together with the LSTP that establishes the secure communications link or tunnel across multiple firewalls.

D. The Fox Reference

Fox describes a secure push server. The push server is used for sending notifications to different wireless clients on different wireless networks. The push server allows information service providers to send notifications to the wireless clients. The information service providers initiate a request to the push server that includes updated information. The request also includes a certificate from the information service provider. The push server authenticates the request from the information service provider by verifying the certificate. The push server also determines if the certificate was issued from an acceptable certificate authority by examining an acceptable certificate authority list. Finally, the push server checks the content of the notification to be sure it does not interfere with other information service providers. After performing the security checks, the push server processes the notification request.

E. The Griffiths Reference

Griffiths describes a system for storing information on a computer network and allowing the information to be accessed by terminals connected to the computer network, either directly, or through an intermediary device such as a local or proxy server, includes computer or web sites which store pages requested by terminals for display on the terminals. The pages may include references to banners to be displayed in conjunction with the web pages on the terminal. The terminal initiates access or connection to a desired computer or web site to access a desired page. After the desired page is downloaded, transmitted, or served to the terminal from the computer or web site, the terminal initiates and sends an initial banner request signal to an information server. The information server returns a redirect signal to the terminal telling the terminal the location of the desired banner on the computer network, which may be the information server, the computer site, or some other information server, computer site, or location accessible via the computer network. The terminal then initiates a second banner request signal to the location of the desired banner and the banner is served to the terminal for display on the terminal, unless the requested banner has previously been stored or cached in the terminal's memory or in the memory of a local or proxy server connected to the terminal, in which case the second banner request signal is not sent across the computer network and the banner is loaded directly from the terminal's memory or served to the terminal from the proxy server.

F. The Coley Reference

Coley describes providing a firewall for isolating network elements from a publicly accessible network to which such network elements are attached. The firewall operates on a stand alone computer connected between the public network and the network elements to be protected such that all access to the protected network elements must go through the firewall. The firewall application running on the stand alone computer is preferably the only application running on that machine. The application includes a variety of proxy agents that are specifically assigned to an incoming request in accordance with the service protocol (i.e., port number) indicated in the incoming access request. An assigned proxy agent verifies the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request.

G. The Raz Reference

Raz describes an information transfer network, comprising: a plurality of client terminals which comprise a presentation system having a control and management agent system; a plurality of servers which comprise a database system and an application system, and a control and management agent system; a request broker system which permits the exchange of information between said client terminals and said servers through a communication path between said terminal and said server, and an information management system for dynamically controlling the location, access and transfer of information between said client terminals and said servers through a plurality of communication paths connecting said control and management agent system of each of said client terminals and servers to said information management system.

H. The Applicants' Claims Are Patentable Over The References

Applicants' invention, as recited in independent claims 1, 40 and 79, is patentable over the references, because the claims recite a specific combination of limitations not found in the references. Specifically, the references do not teach or suggest the specific sequence of steps comprising: (a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network; (b) establishing a Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection; (c) mutually authenticating each of the endpoints of the SSL TCP connection; and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated.

Nonetheless, the Office Action cites Crichton at col. 4, lines 62-66, col. 12, lines 9-15, col. 6, lines 30-39 and col. 2, lines 26-27, and col. 7, lines 3-5 as teaching all of the limitations of the independent claims.

Applicants' attorney disagrees. Specifically, Applicants' attorney asserts that Crichton does not teach or suggest the specific sequence of steps in Applicants' claims.

For example, Crichton does not teach or suggest opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network. Instead, Crichton describes how one endpoint proxy (the client proxy 223) opens a connection with the middle proxy, and then another endpoint proxy (the server proxy 213) opens a connection with the middle proxy. When the middle proxy has two matching connections, it joins the two connections by acting like a transparent pipe, operating in a pass through mode.

In another example, Crichton does not teach or suggest opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network, establishing a Secure Sockets Layer (SSL) over the opened TCP connection, and then mutually authenticating each of the endpoints of the SSL TCP connection. Instead, Crichton merely states that the server and client proxies 213 and 223 perform authentication, but not the sequence in which such authentication occurs. no specific steps claimed

In yet another example, Crichton does not teach or suggest multiplexing other connections through the secure connection once both of the endpoints have been authenticated. Instead, Crichton merely states that the requested resources may include multiplexed channels on an existing tunnel connection, but not the sequence in which such multiplexing occurs.

The remaining references fail to overcome the deficiencies of Crichton. For example, Fox was cited merely for using SSL and UDP; Griffiths was cited merely for resolving domain names; Coley was cited merely for using a bastion firewall host computer; and Raz was cited merely for using multiple Intranets.

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over the cited references. In addition, Applicants' invention solves problems not recognized by the cited references.

Thus, Applicant submits that independent claims 1, 40 and 79 are allowable over the cited references. Further, dependent claims 2-39, 41-78 and 80-117 are submitted to be allowable over the cited references in the same manner, because they are dependent on independent claims 1, 40 and 79, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-39, 41-78 and 80-117 recite additional novel elements not shown by the cited references.

III. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: October 31, 2002

By: _____
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30879.64-US-01